BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(1)

[19] JAPAN PATENT AGENCY (JP)
[12] PATENT GAZETTE (A) No.3-26126

[11] Publication of Patent Application

[51] Int Cl.[4]	Identification mark	Internal Agency Number
H 04 L 9/32		
G 06 K 17/00	V	6711-5B
G 09 C 1/00		7343-5B
		6945-5K H 04 L 9/00 A

[43] Publication date: 4th February 1991
Examination: Not requested Number of Claims: 2 (Total 6 pages)

[54] Title of Invention: Electronic Signature Preparing Device

[21] Patent Application Number 1-159767
[22] Date of Application: 23rd June 1989

[72] Inventor Atsushi Shinpo
General Laboratories, Toshiba Corp., Komuke Toshiba-cho, Saiwai-ku, Kawasaki-shi, Kanagawa Prefecture
[72] Inventor Shinichi Kawamura
General Laboratories, Toshiba Corp., Komuke Toshiba-cho, Saiwai-ku, Kawasaki-shi, Kanagawa Prefecture
[71] Applicant Toshiba Corp.
72 banchi, Horikawa-cho, Saiwai-ku, Kawasaki-shi, Kanagawa, Prefecture
[74] Agent: Hideyoshi Miyoshi, Patent Attorney, and another

SPECIFICATIONS

1. Title of the Invention

Electronic Signature Preparing Device

2. Claims

[Not translated]

3. Detailed Description of the Invention

Relevant field of industry

This invention relates to an electronic signature preparing device that is applicable to information communication systems that employ public key codes, and that securely prepares signatures.

Prior art

The ability to verify the creator of messages that are received, that the message has not been altered from the state in which its creator created it, and that the other party in the

communication is the intended party are important conditions of information communication systems.

The use of encryption techniques, and particularly of public key codes, has been considered as a means providing a verification function in such information communication systems.

Public key encryption such as RSA (Rivest-Shamir-Adleman) encryption is characterized by the use of separate public keys and private keys.

In such cases, each user has a different private key which the user keeps secret, while the public key (which is also different for each user) is held publicly as on a database, and is managed securely in order to prevent tampering.

Thus methods of verification that employ such public key encryption are commonly found in digital signature processes.

With digital signatures, the user creates a signature **S** which the user encrypts and converts by employing the private key and adds such digital signature to the message **M**, as illustrated in Figure 6. The other party then uses the public key to convert the signature **S** back and create the message **M'**, and if the message **M'** matches the message **M** sent by the user, the message **M** that was sent from the user side may be deemed to be the message as created by the user.

It is anticipated that, by means of such digital signature functions, it will in future be possible to provide such services as electronic transactions and funds transfers and so forth through information communication systems.

However, when such services are provided, the user's digital signature will perform the same role as that performed now by a promissory note and the like, and it will be necessary to strictly prevent such actions as the falsification of signatures and illegal (fraudulent) transactions and the like.

For this reason, it is anticipated that the private keys of users will be distributed stored on memory media such as IC cards, to which it is possible to restrict access.

However, at present, the computing capacity of IC cards is not sufficient to provide the private conversion (signature conversion) for RSA encryption and the like, and hence the computing capacity of external terminals such as workstations and personal computers must be employed.

However, it is not desirable that information about private keys be divulged to external terminals.

The dependent computer method has recently been proposed as a method for making temporary use of the computing capacity of an external computer, without divulging information concerning the private key to the external terminal in this fashion (Institute of Electronics, Information and Communication Engineers Research Paper ISEC88-9 and so forth).

By means of this method it is possible to prevent the release of the private key from the IC card to the exterior and to perform the conversion processing at the IC card side alone, whereby it is possible to achieve conversion in secret at high speed.

Moreover, it is considered that, in future, devices that enable high speed conversion in secret will be embedded in the IC cards, which will make it possible to perform the conversion processing in secret at the IC card alone at high speed.

However, even if it should become possible to perform the conversion processing in secret and at high speed without divulging the private key outside the IC card, it is considered that the types of illegal acts described below could be performed from the terminal side.

These procedures are described by relating them to the procedures involved in the creation of an ordinary signature.

First, when the user inserts the user's own IC card in the card reader of the terminal and enters a message **M** for which the signature is to be created from the keyboard of the terminal, or enters the message **M** for which the signature is to be created as an electronic file from the floppy disk drive of the terminal, the terminal sends a different message **M'** from such message **M** to the IC card, and the IC card creates a signature **S'** for the message **M'**.

In this case, the signature is applied to a message **M'** which is different from the message **M** that the user wished to sign.

In other words, the terminal is interposed as an interface between the user and the IC card, and hence the signature could be falsely applied to the message **M'** that the user did not intend.

Terminal switches messages
and another message is signed S'.

Problems addressed by the invention

The user IC card of the prior art as described in the foregoing and as exemplified by the creation of a signature by means of a computing device specific to the user and a terminal makes possible the supply of an illegal signature through the terminal, and hence the development of a system that would completely prevent this has been highly desirable.

The present invention takes account of this situation, and it is an objective of the present invention to provide an electronic signature preparing device that makes possible the complete prevention of illegal acts perpetrated by means of the terminal, and in this manner, greatly enhances the security of signatures.

Constitution of the invention

Means of overcoming such problems

In order to achieve the objective described above, the electronic signature preparing device envisaged by the present invention is characterized by a terminal that is connected to a network, and an electronic signature preparing device that is provided with an individual user computing device that is connected to such terminal, such electronic signature preparing device being provided with a storage part that stores the private key, and an output part that notifies the user of the contents of the message that are supplied from the said terminal, and a signature permission and refusal part whereby the user enters an instruction permitting or refusing the signature, and a calculation part that employs the private key that is stored in the said storage part to prepare the signature for the said message and to send the said message to the said terminal, when an instruction permitting the signature is entered from the said signature permission and refusal part.

Action

In the constitution described in the foregoing, when a message is output from the terminal to the individual user computing device, the output part notifies the user of the contents of such message, and when the user enters an instruction permitting the signature from the said signature permission and refusal part, the calculation part employs the private key that is stored in the storage part and prepares a signature for the message and sends the signature to the said terminal.

Practical embodiments

Figure 1 is a block diagram that illustrates a practical embodiment of an electronic signature preparing device as envisaged by the present invention.

The electronic signature preparing device illustrated in the drawing is provided with an external terminal 1 that consists of a personal computer or the like that is connected to an information communication network, and an IC card reader-writer 2 that is connected to such external terminal 1, and IC card 3 that is employed by the individual user computing device, and when the user inserts the IC card 3 into the IC card reader-writer 2 in order to prepare a signature, the message M to which the signature is to be applied is displayed on the IC card 3 whereby the user may confirm the contents of the message M and perform the action of signature.

In this case, the IC card 3 is provided with a storage part 9 that stores the user's private key and the user's password or the like and the said private key that is stored in the storage part 9 and a calculation part 5 that employs the said private key that is stored in the said storage part 9 and employs portion of the computing capacity of the external terminal 1 through a standalone or dependent computing means to perform high-speed code conversion processing and that displays the message **M** to which the signature is to be attached, and a communication part 6 that electrically connects the said calculation part 5 and the said IC card reader-writer 2 when the IC card 3 is inserted into the said IC card reader-writer 2, and an information output part 7 that displays to the user and so forth the message **M** that is output by the calculation part 5, and a signature preparation confirmation signal input part 8 that operates when the user signs the contents of the message **M** that is displayed in the information output part 7, as illustrated in Figure 2.

Fig. 2

Next, the action of the practical embodiment is described by reference to the flowchart that is illustrated in Figure 3.

First, prior to the action of signing, the user inserts the IC card 3 into the IC card reader-writer 2 (step ST1).

Thereupon, the user operates the keyboard of the external terminal 1 and enters the password, and the external terminal 1 supplies the said password through successively the IC card reader-writer 2 and the communication part 6 of the IC card 3 to the calculation part 5 and then checks whether or not the password matches the password that is stored in the memory part 9 (step ST2).

Next, if these do not match, the calculation part 5 creates a password error message and sends it to the external terminal 1, and a message such as 'Password error' or the like is displayed on the screen of the external terminal 1.

Thereupon, if the correct password is entered within the specified number of attempts, the external terminal 1 enters a message acceptance enabled state.

Thereupon, if the message **M** that is to be signed is entered by operation of the keyboard of the external terminal 1, or by inserting a floppy disk that contains the message **M** into the floppy disk drive of the external terminal 1, or by the selection of the message **M** that has been sent from another terminal in a form such as electronic mail through an information communication network, the external terminal 1 supplies the message **M** that is to be signed through the IC card reader-writer 2 and the communication part 6 of the IC card 3 successively to the operation part 5 (step ST3).

Thereupon, the calculation part 5 supplies the message **M** to the information output part 7 and submits the contents of the message **M** to the user (step ST4).

Next, if the user having viewed the contents of the message **M** that were displayed on the information output part 7 deems it desirable to sign the message **M**, the user presses the confirmation key of the signature preparation confirmation signal input part 8 (step ST5), and the calculation part 5 detects this and employs the private key that is stored in the memory part 9 and performs encryption conversion on the message **M** by means of the standalone

calculation method or the dependent calculation method and prepares the signature S (step ST6).

Thereupon, the calculation part 5 supplies the signature S and the message M that is to be signed that have been obtained by such encryption conversion processing through successively the communication part 6 and the IC card reader-writer 2 to the external terminal 1, and either transmits them to another terminal by means of the information communication network or stores them in the external terminal 1 (step ST7).

Moreover, if during the check processing of the message M described above (step ST5) the user does not press the confirmation key of the signature preparation confirmation signal input part 8 within a specified period of time, or the signature preparation disallowed key is pressed, the calculation part 5 suspends encryption conversion processing and terminates processing.

Thus, in the present practical embodiment, an information output part 7 is provided in the IC card 3 and the message M that is to be signed is displayed in such information output part 7 for confirmation of the contents of the message M by the user, and hence it is possible to completely prevent any illegal act through the external terminal 1 or through another terminal, and hence it is possible to greatly enhance the security of the signature.

Moreover, in the foregoing description of the practical embodiment of the invention, the example described was of the information output part 7 projecting externally from the IC card reader-writer 2 while the IC card 3 was inserted into the IC card reader-writer 2, but if the information output part 7 is within the IC card reader-writer 2 and is not directly visible from the exterior when the IC card 3 is inserted into the IC card reader-writer 2, when the message M is confirmed, the IC card 3 can be withdrawn from the IC card reader-writer 2 whereupon the signature preparation confirmation signal input part 8 can be operated to enter approval or disallowance of the preparation of the signature, whereupon the IC card 3 can be inserted into the IC card reader-writer 2 in order to continue processing.

Moreover, in the foregoing description of the practical embodiment of the invention, an IC card 3 is employed that is provided with a signature approval key and a signature disallowance key, but an IC card 3b such as that shown in Figure 4 may be employed in place of such IC card 3. In this drawing, those parts that are identical with parts in Figure 2 are indicated by the same symbols.

The difference between the IC card 3b that is shown in the drawing and the IC card in Figure 2 is that an information input part 10 that possesses a keyboard or the like is provided in place of the signature preparation confirmation signal input part 8, it being possible to instructions to approve or disallow the preparation of the signature and to enter the contents of the message M by operating the keyboard of the information input part 10.

In this case, the signature is prepared according to the procedures in the flowchart shown in Figure 5.

First, prior to signature operation, the user inserts the IC card 3b into the IC card reader-writer 2 (step ST10).

Thereupon, when the user operates the keyboard of the external terminal 1 and enters the password, the external terminal 1 supplies the said password to the calculation part 5 through successively the IC card reader-writer 2 and the communication part 6 of the IC card 3, and checks whether the password matches the password that is stored in the memory part 9 (step ST11).

Next, if these do not match, the calculation part 5 creates a password error message and sends it to the external terminal 1, and a message such as 'Password error' or the like is displayed on the screen of the external terminal 1.

Thereupon, if the correct password is entered within the specified number of attempts, the external terminal 1 enters a message acceptance enabled state.

Thereupon, the user withdraws the IC card 3b from the IC card reader-writer 3b and operates the keyboard that is provided in the information input part 10 and enters the message M that is to be signed, whereupon the calculation part 5 fetches the message and supplies it to the information output part 7 and submits the contents of the message M to the user.

Next, if the user having viewed the contents of the message M that were displayed on the information output part 7 deems it desirable to sign the message M, the user operate the keyboard of the information input part 10 and enters a signature approval instruction, and the calculation part 5 detects this and sets a signature approved flag in internal memory (step ST11).

Thereupon, the user inserts the IC card 3b into the IC card reader-writer 2 and the calculation part 5 checks whether or not a signature approved flag has been set in internal memory, and if it has been set, employs the private key that is stored in the memory part 9 and performs encryption conversion on the message M by means of the standalone calculation method or the dependent calculation method and prepares the signature S (step ST13)[1].

Thereupon, the calculation part 5 supplies the signature S and the message M that is to be signed that have been obtained by such encryption conversion processing through successively the communication part 6 and the IC card reader-writer 2 to the external terminal 1, and either transmits them to another terminal by means of the information communication network or stores them in the external terminal 1 (step ST14).

In this manner, in the present practical embodiment of the invention, an information input part 10 that possesses a keyboard or the like is provided on the IC card 3b, and instructions for the approval or disallowance of the signature, and the contents of the message M, may be entered through the keyboard of the information input part 10, and hence it is possible to completely prevent illegal acts through the external terminal 1 or through other terminals.

Effects of the invention

The present invention as described in the foregoing is able to completely prevent the performance of illegal acts through terminals, and thereby greatly enhances the security of the signature.

1 Step ST12 not specifically identified in the Japanese text - Translator

(8)

4. Simplified description of the drawings

Figure 1 is a block diagram that shows a practical embodiment of the electronic signature preparing device envisaged by the present invention, Figure 2 is a detailed block diagram of the IC card shown in Figure 1, Figure 3 is a flowchart that shows an example of the operations in this practical embodiment, Figure 4 is a detailed block diagram of an IC card that is employed in a further practical embodiment of the electronic signature preparing device envisaged by the present invention, Figure 5 is a flowchart that shows an example of the operations when the IC card that is shown in Figure 4 is employed, and Figure 6 is a schematic diagram that is intended to explain digital signatures.

1 ... Terminal (external terminal)
2 ... IC card reader-writer
3 ... Individual user calculation device (IC card)
5 ... Calculation part
7 ... Output part (information output part)
8 ... Signature confirmation input part (signature preparation confirmation signal input part)
9 ... Storage part (memory part)

Agent: Hideyoshi Miyoshi

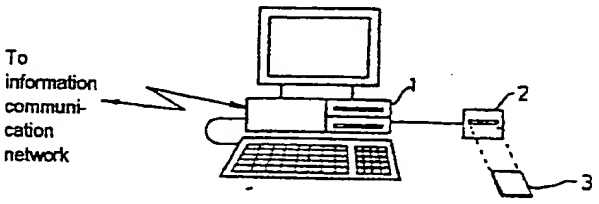

Figure 1

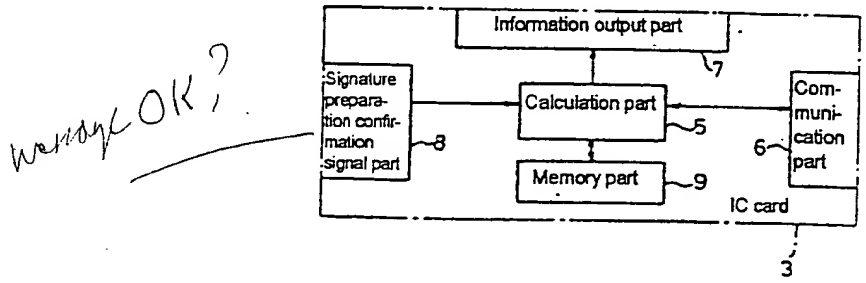

Figure 2

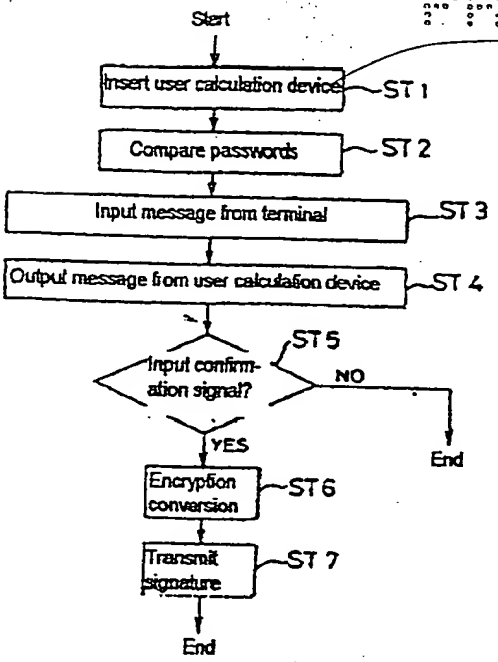

Figure 3

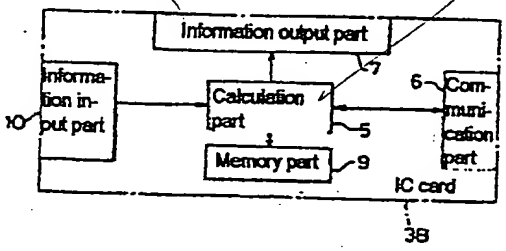

Figure 4

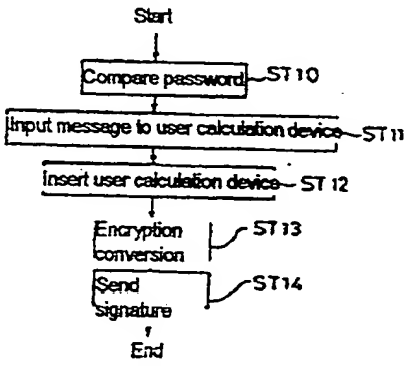

Figure 5

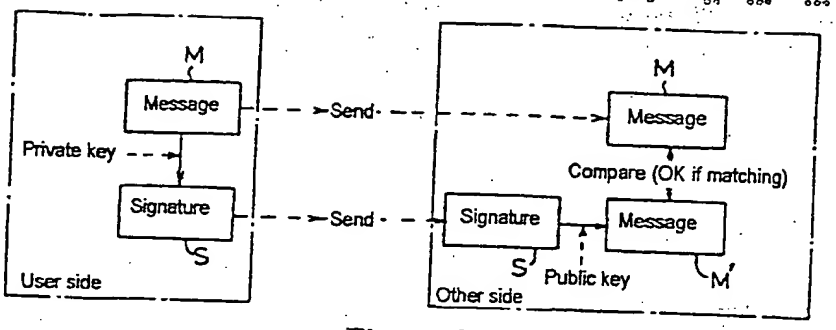
M
Message
Private key
Signature
S
User side
Send
Send
M
Message
Compare (OK if matching)
Signature
Message
S'
Public key
M'
Other side

Figure 6